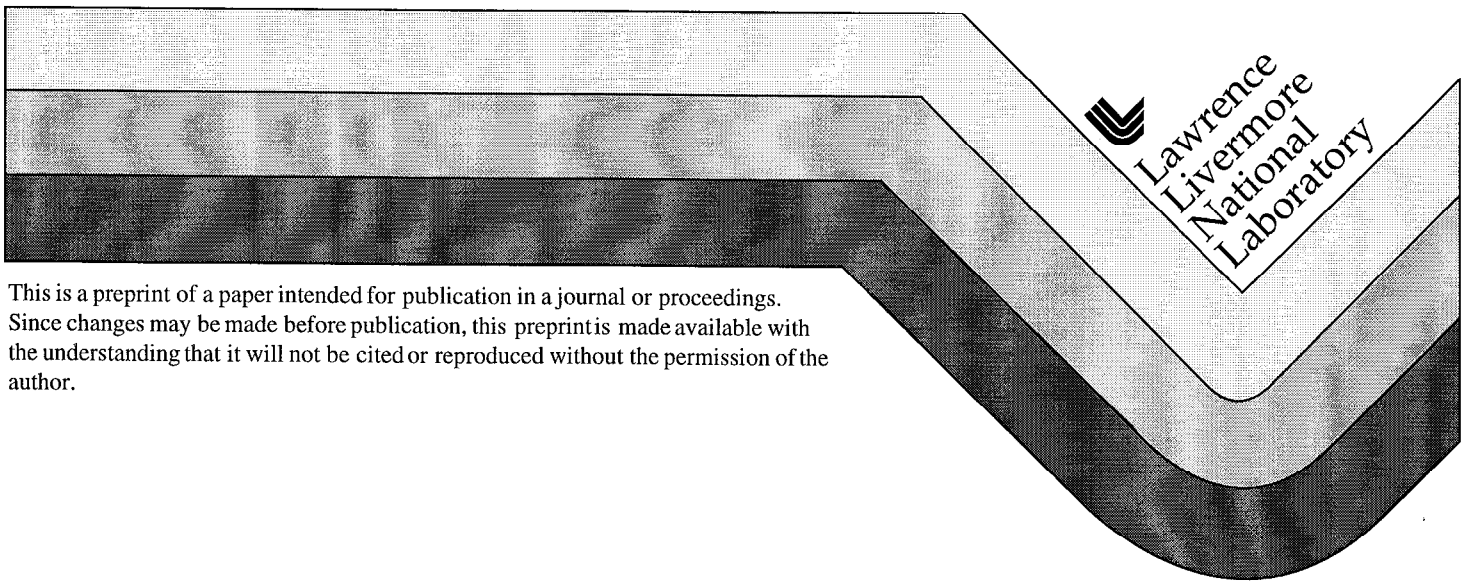
UCRL-JC-133202
PREPRINT

Development of a Safety Interlock System for the National Ignition Facility Optical Line Replaceable Unit Transport and Handling Systems

T. B. Hall

This paper was prepared for submittal to the
8th International Topical Meeting on Robotics and Remote Systems
Pittsburgh, PA
April 25-30, 1999

February 8, 1999



Development of a Safety Interlock System for the National Ignition Facility Optical Line Replaceable Unit Transport and Handling Systems

T. Brett Hall (Lawrence Livermore National Laboratory)
P.O. Box 808, L-447, Livermore, CA 94550
e-mail: hall44@llnl.gov
Tel: (925) 422-3745

ABSTRACT

The National Ignition Facility (NIF) at Lawrence Livermore National Laboratory (LLNL) is developing a distributed control system called the Operations Engineering Special Equipment Control System (OSECS). The OSECS will support semi-autonomous and autonomous transport of Line Replaceable Units (LRUs) using automated guided vehicles. In addition, OSECS will support the assembly, and disassembly of LRUs in the NIF Optics Assembly Building (OAB). The OSECS consists of approximately 4,000 control points, 35 Front End Processors (FEPs), and a Supervisory System. This design must be highly reliable and maintainable over a 30-year lifetime. Supporting the OSECS installation systems is a Safety Interlock System (SIS) that will ensure personnel and equipment safety during operations. The SIS is a stand-alone Programmable Logic Controller (PLC) based system on-board the delivery system.

The subject of this paper is the SIS requirement research and the SIS design and integration into the delivery system. Because the SIS is safety related, it is a fully separate system from the local control FEP that will control the motors, actuators, and other systems. The necessary level of safety is achieved by providing permissive signals for the operation of motors and other equipment within the systems. The SIS will also monitor the crash buttons located on each delivery system. When these are pressed, power will be removed, stopping all motions. This action should immediately provide safe conditions around the delivery system. The SIS will also be required to make status reports. It will report status to the OSECS supervisory system, which will be controlling and keeping track of the delivery systems. This status will be communicated via ethernet to the on-board FEP, where it will then be communicated over a wireless network to the supervisory server. Here it will be displayed on the supervisory graphical user interface displays. This will keep the supervisory system informed of the state of the SIS. The resulting SIS design is a robust, flexible, and scalable environment aptly suited to keep OSECS operations safe through the 30-year life expectancy of the NIF.

1. Introduction

The National Ignition Facility (NIF) is a large-scale inertial confinement laser fusion facility which will be located on-site at Lawrence Livermore National Laboratory (LLNL) in Livermore, California. The NIF is the first project in the US Department of Energy's Stockpile Stewardship program, and will enhance current laser research and will provide insight into development of a productive fusion power plant. The

NIF is a 1.2 Billion-dollar project that will house the world's largest laser, and will be approximately the size of a football stadium when finished in 2003. NIF Operations Engineering is developing several Transport and Handling (T&H) systems which will be used to install laser optics (called Line Replacable Units or LRUs) into the NIF laser. Controlling these T&H systems is the Operations and Special Equipment Control System which consists of several levels of control computers and a Safety Interlock System (SIS) which resides on the T&H delivery systems. The SIS is a safety shut-down system which will ensure that the delivery systems are operated safely and will protect operations personnel from harm. The SIS will also protect against significant equipment damage on the delivery systems, helping to maintain the high availability of these systems. The intent of this paper is to describe the process used to define the Safety Interlock System, and describe the system design and it's interfaces to other systems. This paper is not intended to go into detailed circuit analysis, programming logic, or other low level details to conserve space and maintain a smooth, concise explanation.

2. Background

2.1 National Ignition Facility at LLNL

The NIF is the first project in the US Department of Energy's Stockpile Stewardship program. In an age where nuclear testing is no longer acceptable, other methods must be found to reliably maintain the U.S. stockpile of nuclear weapons. The NIF will be a research facility capable of performing high energy laser experiments which will benefit many other areas of science in addition to fusion research. The NIF is one of the key elements of the Inertial Confinement Fusion Research Program in lasers at LLNL. The goal of NIF is to achieve "ignition" or break even in a fusion reaction with the energy produced equalling or exceeding the energy used to create ignition.

2.2 Transport and Handling

Throughout the operation of the NIF, there are multiple types of laser components (for example laser mirrors) which must be installed, kept clean, removed and refurbished. The NIF transport and handling (T&H) system for handling of these components (called LRUs) will consist of an automated guided vehicle (AGV) and several delivery systems, (see figure I) which will support the installation, removal, and transportation of the various LRUs. The AGV (which is much like a forklift, but smarter) will carry three different types of delivery systems that will insert and remove various types of LRUs; these three types are named by the direction of LRU insertion/removal. The bottom loading canister inserts and removes the LRUs upward into the structure from underneath. A crane picks up the top loading canister and lowers it on top of the laser structure to lower the LRUs in place. The side loading skid (as you may suspect by now) inserts it's LRUs into the structure from the side of the structure.

On-board these delivery systems Front End Processors (FEPs) operate the delivery system mechanisms and communicate to the distributed OSECS supervisory system. Control of these FEPs and delivery systems will be accomplished using mobile handheld computers also communicating to the OSECS supervisory system over a wireless network. The Safety Interlock System (SIS) is a stand alone Programmable Logic Controller (PLC) based safety shut-down system residing on-board the delivery systems to provide personnel & equipment protection local to the delivery system. This safety is provided through a combination of local interlocks and permissives.

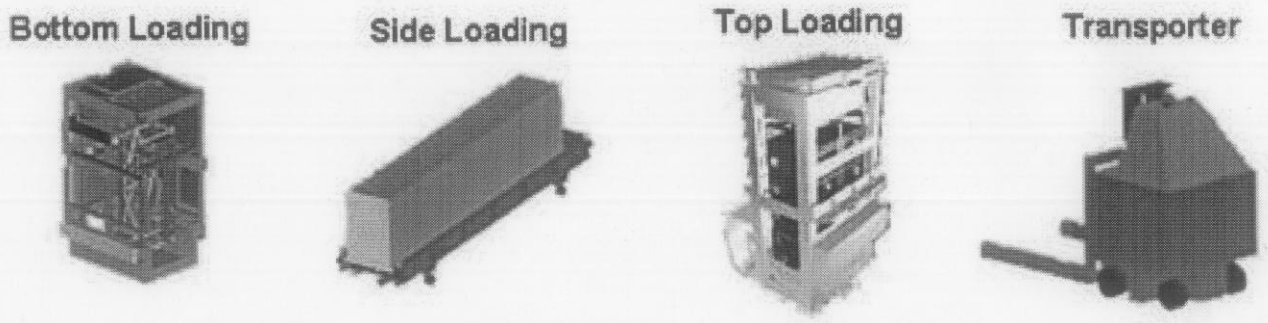


Figure I: T&H Delivery systems and AGV (Transporter)

2.3 Operations and Special Equipment Control System (OSECS) Architecture

The OSECS is a distributed control system that will operate the delivery systems, coordinate the AGV operation, and maintain and archive device status. It consists of multiple control FEPs, multiple SIS FEPs, (one on-board each delivery system), multiple mobile handheld operator computers, and a supervisory system. The OSECS also includes workstations in the Optics Assembly Building (OAB) which will assist in LRU assembly. (see figure II) A wireless Local Area Network (LAN) in the laser bay will enable the AGV, delivery systems, and mobile operator computers to connect to the network while moving around the laser building. The OSECS must be maintainable over the 30-year lifetime of the NIF, and be highly available and reliable to respond to the predicted LRU maintence schedule.

The heart of the OSECS is the supervisory server, which will act as a dispactcher for control requests. The mobile operator computers will issue control events over the wireless network to the supervisory server, where the server will issue the commands to the FEP for the appropriate delivery system. Using this architecture, the supervisory system is aware of the status of devices, and will use a request/subscribe methodology to keep other machines and clients informed about the system state.

One of the strengths of this distributed system is it's ability to have multiple levels of control and status information handled on different computers. This will allow flexibility in the operation of these systems, and will speed the recovery process from a failure.

The SIS fits into this architecture at the FEP level. The SIS physically sits on-board the delivery systems alongside the FEP where it will monitor it's local interlocks and permisssives. The status of the SIS will be sent to the FEP, where it is then transmitted over the wireless to the supervisory server. This will allow the supervisory system to alert an operator about a safety problem quickly, and begin correcting the problem immediately.

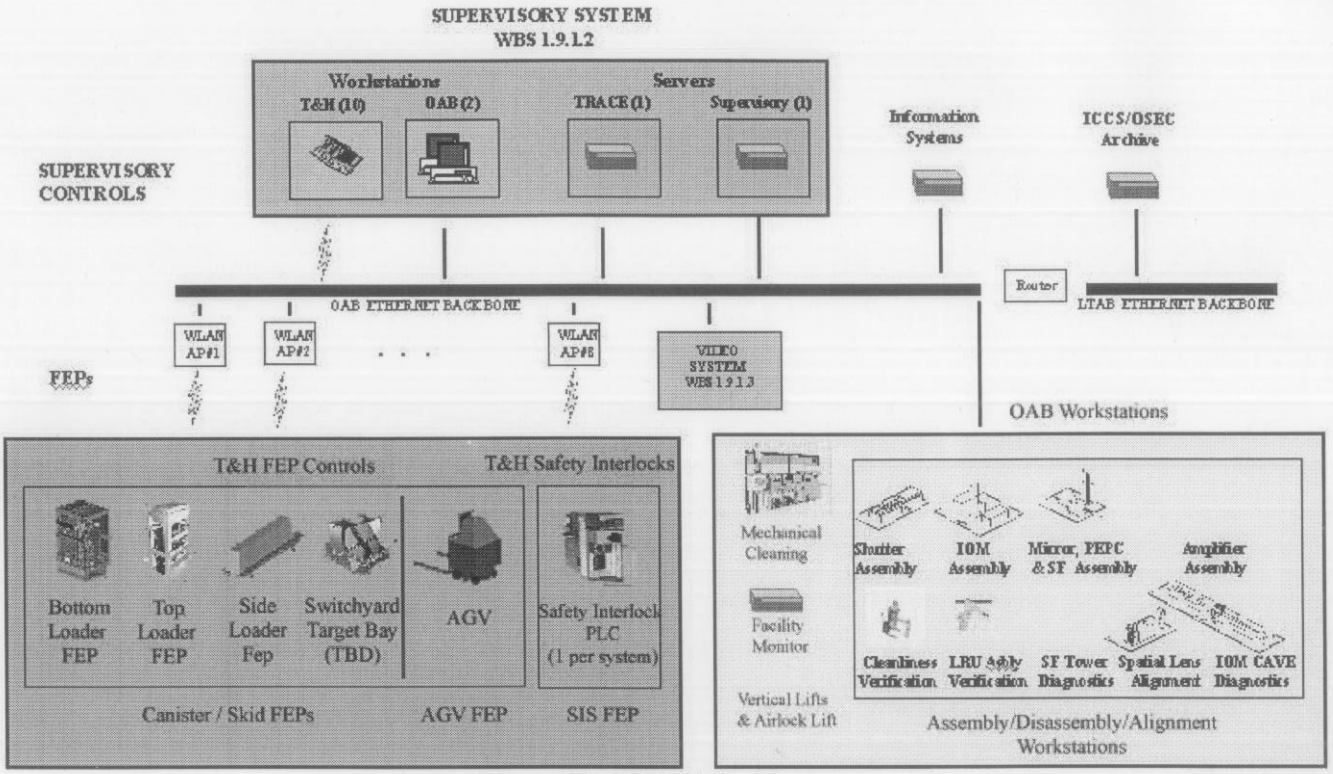


Figure II: OSECS Architecture

2.4 Safety Philosophy

One of the key elements in designing the SIS was defining a philosophy to abide by in making decisions. Being a young engineer (1 yr since B.S. when I started this project) and having never built a safety system before, it was important for me to gain a clear understanding of how safety systems are researched, designed, and built. A critical part of this process was spending time with some experienced safety system designers, and asking them questions on how to go about defining and building the SIS. I was fortunate to gain the assistance of a very experienced engineer who is responsible for building the NIF facility safety system. This relationship also provided an important link that would help maintain a common safety system design across NIF. After asking a lot of questions and learning how LLNL standards effect safety system implementation, I developed a process to define the T&H safety system. The process is summarized in figure III.

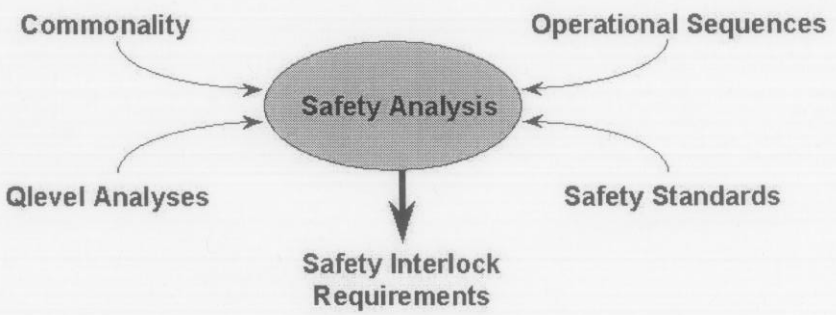


Figure III: Approach to define requirements for the SIS

This process required information gathering from many different people including safety represenatives at LLNL, other NIF safety system designers, T&H control system engineers, and NIF quality control staff (Qlevel is a measurement of Quality requirements). The requirements that were decided upon derived from these meetings. One of the important functions these meetings had besides defining my requirements was provoking discussion among members of teams that normally didn't work together. These discussions lead to items which had not been previously considered; defining the SIS brought many people together to help solve the challenges at hand.

In defining the SIS requirements I encountered two key concepts that drove the SIS design in it's protection of personnel and equipment. In safety systems a *permissive* is defined as a signal which allows or disallows another system to control the output of a device, i.e. the system giving the permissive does not directly control the device. In the SIS permissives are most often used to protect equipment from damage. Also for this system an *interlock* is defined as a category of interaction which occurs in non-regular or emergency conditions in which a potentially dangerous situation will directly result in a system being shut down (or otherwise made safe) creating a safe environment for personnel immediately. In the SIS interlocks are used in situations where personnel may be exposed to a hazard.

Some of the key philosophies we identified and used to define the requirements and design of the SIS follow.

Safety and control systems should be seperated. At LLNL and in most industries it is a standard to require a separate system from the control system to monitor and provide safety in situations where personnel safety is at risk. This provides a level of redundancy, when the normal control system makes a mistake – an independent safety system will make a judgement if the system is fit for continued operation.

Interlocks are never relied upon as the primary means of protection, i.e. they should not be used as part of the normal operating procedure. For example in a typical facility style interlock system which will shut down the exposed voltage behind the panel if the panel is opened, the operator should ensure the power is off and "locked out" before attempting to open the panel. The interlock system will shut off the power as a last resort if the panel is opened with power still on, but this should not be the normal operating mode.

Engineering with safety in mind should also be employed, in that the system's operation should not normally allow unsafe situations to exist. It is tempting to believe that since a system is being carefully watched by a safety system, the normal control system does not need to provide a high level of safety. This is an unsafe way to proceed, but it can be difficult to recognize this when conceptualizing an operation mode. We strove to have diagnostics within the FEP systems using "machine interlocks" (which are interlocks provided by the control system, not by an external system) to make sure that the system operates safely. The SIS should be redundant to provide a very high level of confidence that the system will operate safely.

Reliability is a key component of any safety system. The system and components should be chosen based on good reliability ratings and proven technologies. I am not aware of a direct requirement of this type on safety systems, but common sense indicates that a system whose failure can injure personnel should be held to the highest level of reliability. This filters down into almost all of the system design requirements, including how sensors and relays are connected to the safety system. In addition to the individual component reliabilities, the sensors and relays as the "eyes and ears" of a safety system should also be *connected* in a reliable way. To ensure the highest level of reliability and deterministic failure modes, signals should be directly wired and not communicated over any type of network.

3. Safety Interlock System

3.1 Requirements

In addition to the general requirements for safety systems which have been mentioned in the "philosophy" section, other factors more specific to the details of this system also affected the SIS design. The SIS design will utilize the same PLC platform as the NIF facility safety, which will reduce the inventory of spare parts that must be maintained to support the NIF. It will also simplify maintenance activities, as maintenance personnel will only need to be trained on one PLC platform. Another key factor in the design of the SIS is the need to fit within the tight space allocations in the delivery system control housings.

The specific requirements for the T&H SIS that came from the requirement definition process are summarized as follows:

- Monitoring E-Stops (Crash buttons) on the delivery systems and shutting down the effected systems
- Preventing personnel hazards by safely handling interactions with the AGV and delivery system
- Protecting against damage to LRUs and internal delivery system mechanisms
- Communicating SIS events to the supervisory system for status, archiving, and diagnostics

3.2 Design

A key component of the SIS design is the choice of PLC platform. The new Allen-Bradley ControlLogix PLC platform was chosen for several reasons including it's high reliability and availability, modularity to enable quick hardware changes, small form factor to fit within the controls housing, and it's commonality with the NIF facility system. Since the platform is rather new as of late 1998, we can expect it to be well supported from AB for many years – and we get the advantage of some extra flexibility that the platform supports. The SIS will use this PLC's input and output modules to monitor sensors placed within the delivery systems and provide permissives for operation of the motors in the delivery system. Some of the input/output lines will be dedicated to overseeing the transporter interactions as well, ensuring safe operation. This PLC will also use a serial line to connect to the FEP and transmit status information to the supervisory server for reference and archiving.

Of key importance in designing the SIS is application of the way a permissive works. Figure III contains a typical permissive circuit. The T&H FEP normally controls the servo motor directly, however when a motor permissive is implemented the logic solver (in our case a PLC) has a relay in series with the control signal line. (This is a representation of the actual implementation, the signal line can be a device control signal or power line – the concept is the same. Perhaps it is easier to understand as a power signal.) This will behave such that the FEP can only control the motor when the relay is closed; anytime the relay is opened the motor stops. This is a fail-safe design, in case power in the system is lost, the normally open relay will open causing the motor to stop (go to it's safe state) even if the FEP continues to command it to move. So only when the PLC is powered and specifically allowing motor operation by closing the relay can the motor move.

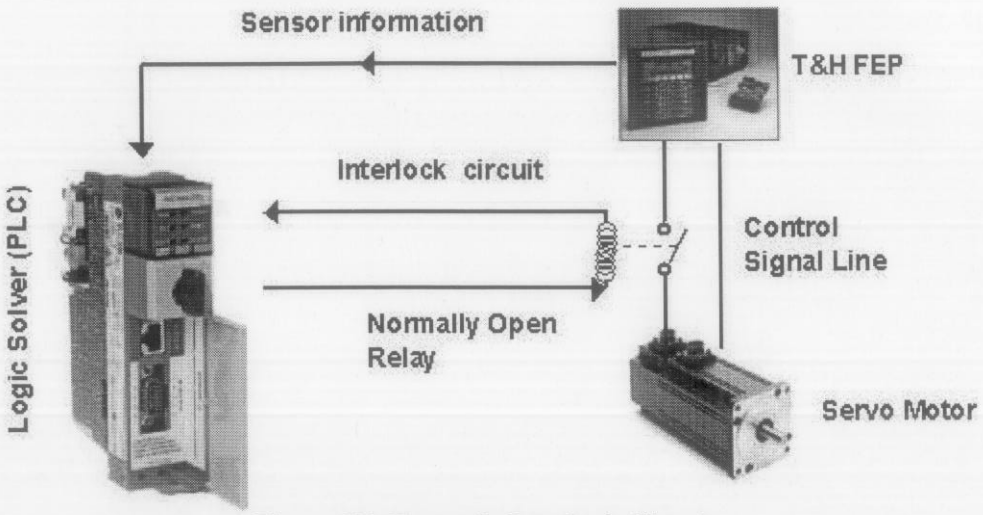


Figure III: Example Interlock Circuit

The SIS will monitor Emergency stop (E-stop) buttons on the outside of the delivery systems. These buttons will immediately halt all system movement when pressed, and will require operator intervention to the SIS to re-enable the system. The circuit to support this involves having the SIS E-Stop buttons wired in series to a relay that delivers all power for the delivery system drive amplifiers, motors, and brakes. These brakes are fail safe and will brake (engage) when power is removed. Note that this circuit is not wired through the PLC, although the PLC will monitor the line to see when the E-Stop has been pressed this is a hard-wired circuit. This relay is wired such that only when the E-Stop is not pressed will power be delivered to the drive amplifiers, motors, and brakes. When an E-Stop button is pressed the relay is de-energized – directly removing power to the aforementioned systems (and engaging the brakes). This results in an immediate halting of system movement, which is not self-resetting. If the E-Stop button is pulled back out the system will not be active again, operator intervention is required at the PLC to reset the system after the cause for the E-stop has been addressed.

Since the AGV will carry the delivery systems during most operations, having separate E-stops for both systems is a source of potential operator confusion and inconvience. This potential problem is compounded by the fact that at times the delivery system may be 10 feet up in the air, and personnel would be unable to reach the delivery system E-stop. To eliminate this issue, the E-stop systems will be connected in series such that an E-stop on either the AGV or the delivery system will halt all operations on both systems. This E-stop is carried through individual signal wires contained in a cable physically connected between the AVG and the SIS. Power to the internal SIS PLC, FEP computer, and airflow systems (recirculation system maintaining a clean room environment inside the delivery systems) will be left on during an E-stop condition, as they do not pose a safety hazard. Leaving the computers running (but disabling the hardware directly) will also assist in diagnostics and recovery from an E-Stop condition and help eliminate unecessary down time.

In addition to the E-stop buttons on both the AGV and delivery system being in series, simultaneous operation of both systems will not be allowed; only one system shall be in control at any one time. In order to implement this, the SIS will monitor a set of signals in the cable between the two systems to make sure that both systems will comply. A request/acknowledge control handoff protocol on distinct lines of the cable will be used to determine which system is in operation, and ensure that only one is in operation. If the SIS detects that both systems are running at the same time, it will E-stop both systems.
Since the proper operation of the E-Stops and control handoff relies on this cable, it must be in place when the AGV and delivery systems are together. This will be ensured through use of an SIS sensor located on the delivery system detecting when an AGV is present – anytime an AGV is present the SIS will not allow movemement until the cable is connected.

A system of permissives for operation of the motors has been developed to protect against damage to LRUs and other equipment within the delivery systems. The SIS gives permission for motor operation by individually enabling or disabling each servo drive amplified and allowing the FEP to operate the brakes. Anytime the SIS determines that it is unsafe for the motor to operate it will remove the permissive (disabling motor operation) and engage the brakes. A specific sensor or set of sensors will be monitored to determine the state of the system, often involving limit switches on the different mechanisms. There is one exception to this general rule, one of the sub-systems in the Bottom Loader delivery system uses pneumatic control. In this system, the SIS will only close a valve (allowing system motion) when it is safe for the operation of this device. Any other time this valve will be open making sure the system cannot move.

Status information from the SIS will be communicated over a serial communication line with the FEP. Allen-Bradley RSLinx software running on the FEP will interpret the communication from the PLC and use a DDE prototcol to communicate this information to the supervisory client also running on the FEP. This client will then send the information in the form of events up to the supervisory server.
Note: This communication is not absolutely necessary for SIS operation. The SIS shall be capable of running "stand alone" with or without the communications cable.

4. Conclusions

The OSECS system will provide a flexible and reliable T&H control system for maintaining NIF over it's 30 year lifespan. The SIS safety shutdown system is a key component of the operation of these T&H systems, ensuring that operations are reliable, safe for personnel, significant damage does not occur. The SIS requirement gathering process and design has brought many individuals on different teams together in thinking about how to make the operations safe, in addition to ensuring a successful SIS. An important early step in the SIS development was understanding the philosophy to guide the safety system design through difficult decisions in the requirement and design phases. The thorough requirement gathering process ensured that the design would meet industry and LLNL standards, and provide safety on the right sub-systems in the T&H equipment. The SIS design relied heavily on reliable and robust long-term operation, utilizing a well-proven PLC common to NIF. The implementation of the lowest level sensors and relays is key to how the system finally functioned, and has been designed to be consistent with the well thought out requirements. The SIS design is being prototyped along with the first-off T&H systems and has been a success in all tests so far, we expect similar success in the other systems which will be finished with prototyping in mid 1999. Ultimately the robust design of the SIS will enable safer NIF T&H operations, assisting LLNL and the Department of Energy strive to reach their goals of enhancing laser technology and fusion research through the NIF.

ACRONYMS

The following acronyms are used in this document:

NIF: National Ignition Facility

OSECS: Operations and Special Equipment Control System

T&H: Transport and Handling

AGV: Automated Guided Vehicle (also called Transporter)

LRU: Line Replaceable Unit

FEP: Front End Processor

SIS: Transport and Handling Safety Interlock System

PLC: Programmable Logic Controller

E-Stop: Emergency Stop

OAB: Optics Assembly Building

LAN: Local Area Network

ACKNOWLEDGEMENTS

I would like to thank many people for their help with the SIS, it has been a collaborative effort that could not have happened without the dedication of many people. Bob Reed (LLNL) has been a tremendous help in understanding industry standard practices for safety, and assisting with early requirements and design. Mike Zimmerman has been making this system happen in our prototyping and yet somehow continues to enforce the ideals that we started in the early design phases. Erna Grasz has been an amazing mentor in electrical engineering at LLNL and has given me the chance to enhance my skills and to be successful on this project. The NIF Operations Engineering controls group including Jo Sander, Donn McMahon, Mark Perez, Dennis Silva, John Laycak, Olaf Koch, Ray Abounader, Ray Iaea, Ed Howe, and Joe Silveira have given me a tremendous base of support in helping me to understand the different systems and being flexible despite the difficulties involved with integrating the SIS into their systems.

REFERENCES

1. Safety Interlock System Requirement Specification NIF5000888

2. Perez, Mark (1999), "Using Embedded Systems for the Remote Delivery and Recovery of National Ignition Facility Optical Line Replaceable Units," *Proc. ANS 8th International Topic Meeting on Robotics and Remote Systems*, Pittsburgh, Pennsylvania, April 25-29, 1999, CD-ROM, American Nuclear Society, La Grange Park, Illinois (1999).

3. McMahon, Donn (1999), "Development of an Automated Guided Vehicle System for Large Scale Materials Handling of Optics in the National Ignition Facility," *Proc. ANS 8th International Topic Meeting on Robotics and Remote Systems*, Pittsburgh, Pennsylvania, April 25-29, 1999, CD-ROM, American Nuclear Society, La Grange Park, Illinois (1999).

4. Tizauer, Detlev; Yakuma, Steve, McMahon, Donn (1999), "A Six Degrees of Freedom End Effector Places 8000lb. Robotic Canisters in the National Ignition Facility," *Proc. ANS 8th International Topic Meeting on Robotics and Remote Systems*, Pittsburgh, Pennsylvania, April 25-29, 1999, CD-ROM, American Nuclear Society, La Grange Park, Illinois (1999).

5. Gruhn, Paul; Cheddie, Harry, "Safety Shutdown Systems: Design, Analysis and Justification, Instrument Society of America, Research Triangle Park, North Carolina, 1998

This work was performed under the auspices of the U.S. DOE by LLNL under contract No. W-7405-Eng-48.